REMARKS

The Office Action dated January 22, 2009, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 10-11, 23, and 65 have been amended to more particularly point out and distinctly claim the subject matter of the invention. No new matter is added. Applicants submit claims 1-31, 42-43, and 62-65 for consideration in view of the following.

Claims 1-31, 42-43, and 62-65 were rejected under 35 U.S.C. § 102(e) as being anticipated by RFC3261 (SIP: Session Initiation Protocol) (hereinafter "RFC"). It should be noted that this rejection is improper because a rejection under 35 U.S.C. § 102(e) can only be proper when the references relied upon are patents, patent applications, or patent publications. In the instant case, the rejection does not rely on such a document. Consequently, the rejection is improper on its face. Therefore, Applicants respectfully request that this rejection be withdrawn and that a new, non-final Office Action be issued, or, in the alternative, that the pending claims be allowed.

Additionally, Applicants respectfully point out that none of claims 1-31, 42-43, and 62-65 are anticipated by RFC for at least the following reasons.

Claim 1, upon which claims 2-11 and 43 depend, recites a method that comprises receiving a message at an interrogating call session control function using a public service identity. The method also comprises obtaining address information for a network

function for which the message is intended. The method further comprises sending the message to the network function in accordance with the address information.

Claim 12, upon which claims 13-20 depend, recites a method that comprises originating a message from a network function using a public service entity, determining an address of a proxy entity to which the message is to be sent, and routing the message to the proxy entity, wherein the message is routed from the proxy entity to an entry point of a target network.

Claim 22 recites a method that comprises originating a message from a network function using a public service entity, determining an interrogating call session control function to which the message is to be sent, and routing the message directly to the interrogating call session control function when the interrogating call session control function is in a same network as the network function.

Claim 23 recites a method that comprises originating a message from a network function using a public service identity, determining the interrogating call session control function to which the message is to be sent, and routing the message directly to the interrogating call session control function when the interrogating call session control function is in a trusted network.

Claim 24, upon which claims 25-27 depend, recites a method that comprises receiving a request from a network function at an interrogating call session control function using a public service entity, determining, at the interrogating call session control function, a serving call session control function to which a message from the

network function is to be sent, and sending the message to the determined serving call session control function.

Claim 28, upon which claims 29-31 depend, recites a method that comprises receiving a request from a first network function at an interrogating call session control function using a public service identity, determining, at the interrogating call session control function, a second network function to which a message from the first network function is to be sent, and sending the message directly from the interrogating call session control function to the second network function.

Claim 42 recites a method that comprises receiving a message at an interrogating call session control function from a network function based on address information obtained by the network function using a public service entity, obtaining address information at the interrogating call session control function for the message, and sending the message from the interrogating call session control function in accordance with the address information.

Claim 62 recites an apparatus that comprises means for receiving a message using a public service entity, means for obtaining address information for a network function for which the message is intended, and means for sending the message to the network function in accordance with the address information.

Claim 63, upon which claim 64 depends, recites an apparatus that comprises a receiver configured to receive a message using a public service entity. The apparatus also comprises an address information entity configured to obtain address information or

a network function for which the message is intended. The apparatus further comprises a transmitter configured to transmit the message to the network function in accordance with the address information.

Claim 65 recites a computer program embodied on a computer-readable medium. The computer program is configured to control a processor to perform operations that comprise receiving a message at an interrogating call session control function using a public service entity. The operations also comprise obtaining address information for a network function for which the message is intended, and sending the message to the network function in accordance with the address information.

Each of claims 1-31, 42-43, and 62-65 recites limitations that are not disclosed or suggested by RFC.

RFC discloses Session Initiation Protocol (SIP). In RFC, an application-layer control (signaling) protocol is presented for creating, modifying, and terminating sessions with one or more participates. The sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. Additionally, SIP invitations are used to create sessions and to carry session descriptions that allow participates to agree on a set of compatible media types.

However, RFC fails to disclose or suggest all the limitations of any of claims 1-31, 42-43, and 62-65. For instance, RFC fails to disclose or suggest "receiving a message at an interrogating call session control function using a public service identity," as recited in claim 1, and as similarly recited in claims 24, 28, 42, 62-63, and 65. Additionally, RFC

fails to disclose or suggest "originating a message from a network function using a public service entity," as recited in claim 12, and as similarly recited in claims 22-23.

Instead, RFC discloses the use of private user identities to establish a communication session. For instance, RFC discloses an SIP message exchange between two users, Alice and Bob (RFC, page 11, paragraph 2, and figure 1). To begin, Alice uses an SIP application on her PC to call Bob using "his" SIP identity (RFC, page 11, paragraph 3). An example of Bob's SIP identity is a personalized series of characters such as "sip:bob@biloxi.com," where "bob" is a user display name and "biloxi.com" is a domain of Bob's SIP service provider (RFC, pages 12-13). Accordingly, RFC discloses a communication establishment process that relies on private user identities that identify a private user, which is not a public service, for example.

By contrast, the public service identities used by the claimed invention can identify services that are hosted by application servers capable of executing service specific logic corresponding to the public service identity. (See, e.g., Application, page 49-50). Further, the use of public service identities, as opposed to private user identities, can enable a request to always be routed via a CSCF, an S-CSCF, a destination network, and/or according to operator decision, as opposed to being routed to a user according to a private user identity, for example (See, e.g., Application, pages 50-51). RFC does not describe the private user identities as enabling any of these functions or capabilities. Consequently, RFC fails to disclose "receiving a message at an interrogating call session control function using a public service identity" or "originating a message from a

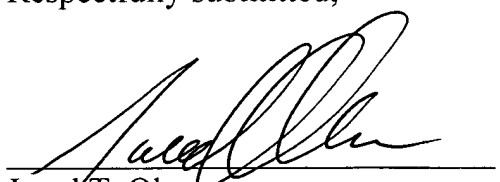
network function using a public service entity," as recited by the rejected claims. Moreover, not only does RFC fail to disclose receiving a message at an interrogating call session control function using a public service identity, but it would be impossible for RFC to do so because RFC fails to contemplate, let alone suggest, the use of public service identities.

Accordingly, RFC fails to disclose or suggest all the limitations of any of claims 1, 12, 22-24, 28, 42, 62-63, and 65. Similarly, RFC fails to disclose or suggest all the limitations of any of claims 2-11, 13-21, 25-27, 29-31, 43, and 64, for their dependence from claims 1, 12, 24, 28, and 63, and for the patentable subject matter recited therein. Consequently, event if RFC were asserted under any of the other paragraphs of 35 U.S.C. § 102, RFC would still not anticipate any of claims 1-31, 42-43, and 62-65. Therefore, Applicants respectfully request that this rejection be withdrawn, and that the pending application be allowed.

If for any reason the examiner determines that the application is not now in condition for allowance, it is respectfully requested that the examiner contact, by telephone, the Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Jared T. Olson
Registration No. 61,058

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

JTO:skl